API SECURITY GUIDELINES AND BEST PRACTICES

Prabath Siriwardena
Senior Director - Security Architecture
prabath@wso2.com | prabath@apache.org

MANAGED APIs

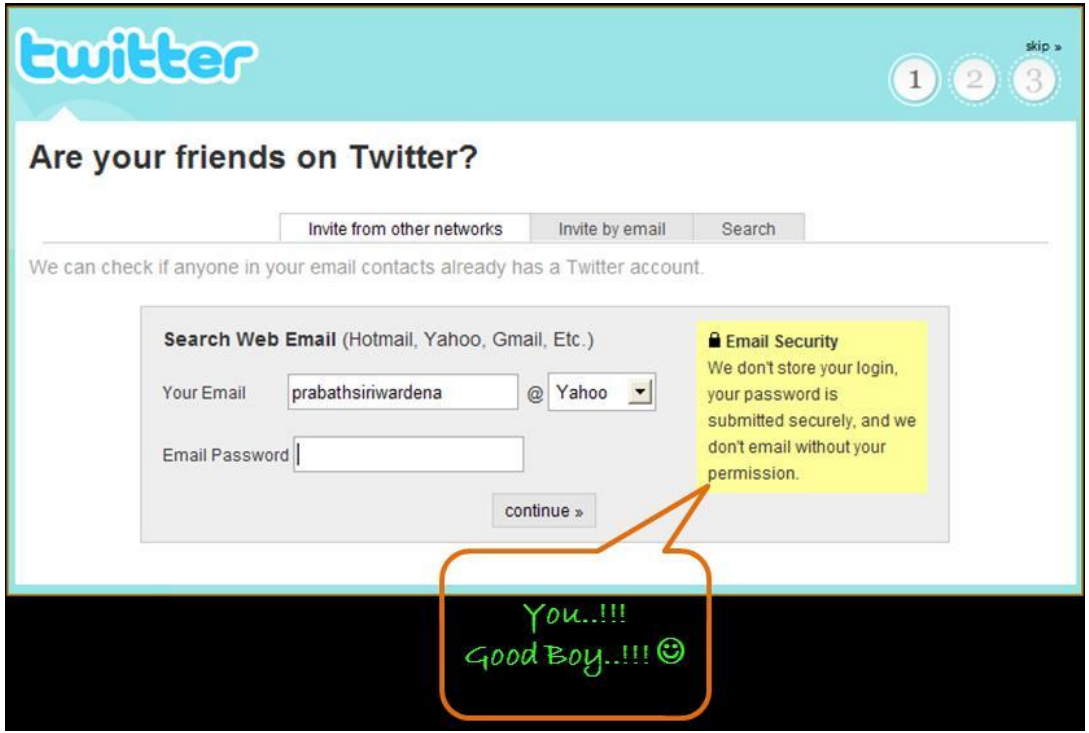
- Secured / Throttled / Monitored / Versioned
- Private vs. Public
- API as a product

OAUTH 2.0

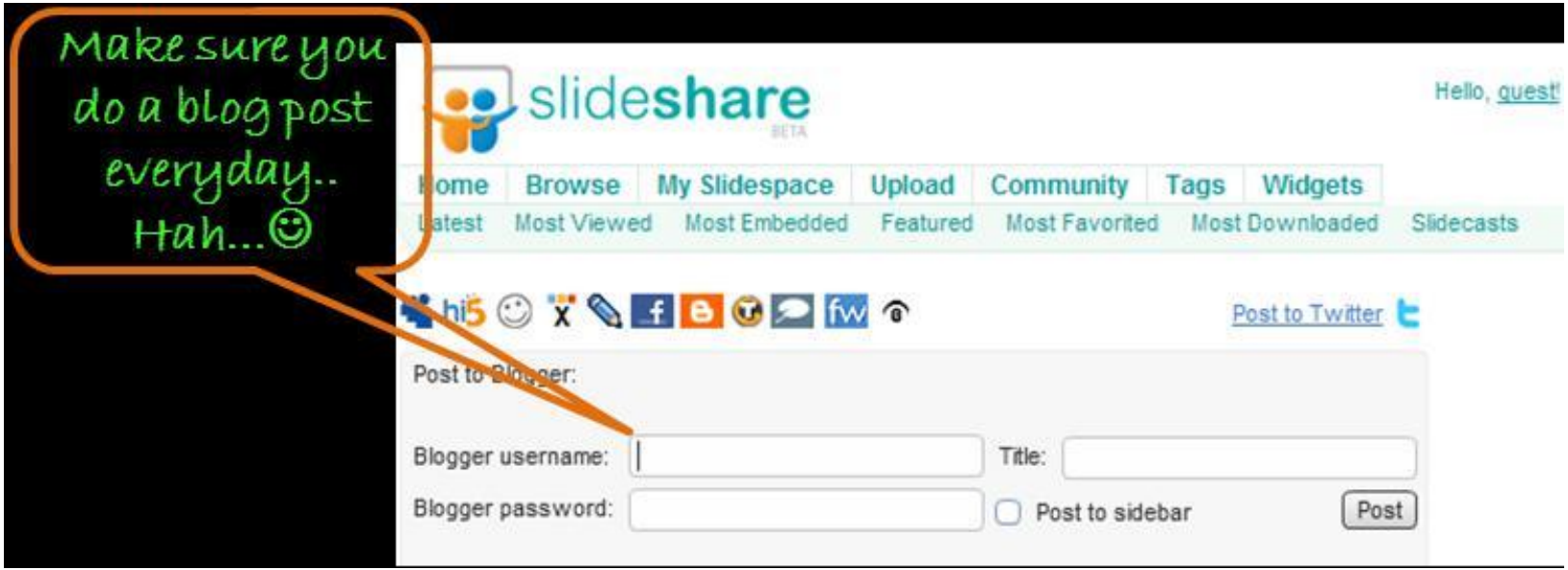
OAUTH 2.0 & ACCESS DELEGATION

- OAuth 2.0 provides a way of delegating access to a third party to access a resource on behalf of the delegator.
- Access delegation via credential sharing (pre-OAuth Era)
- Access delegation via no credential sharing (non-standardized)
- Access delegation via no credential sharing (standardized)

PRE-OAUTH ERA



PRE-OAUTH ERA



PRE-OAUTH ERA

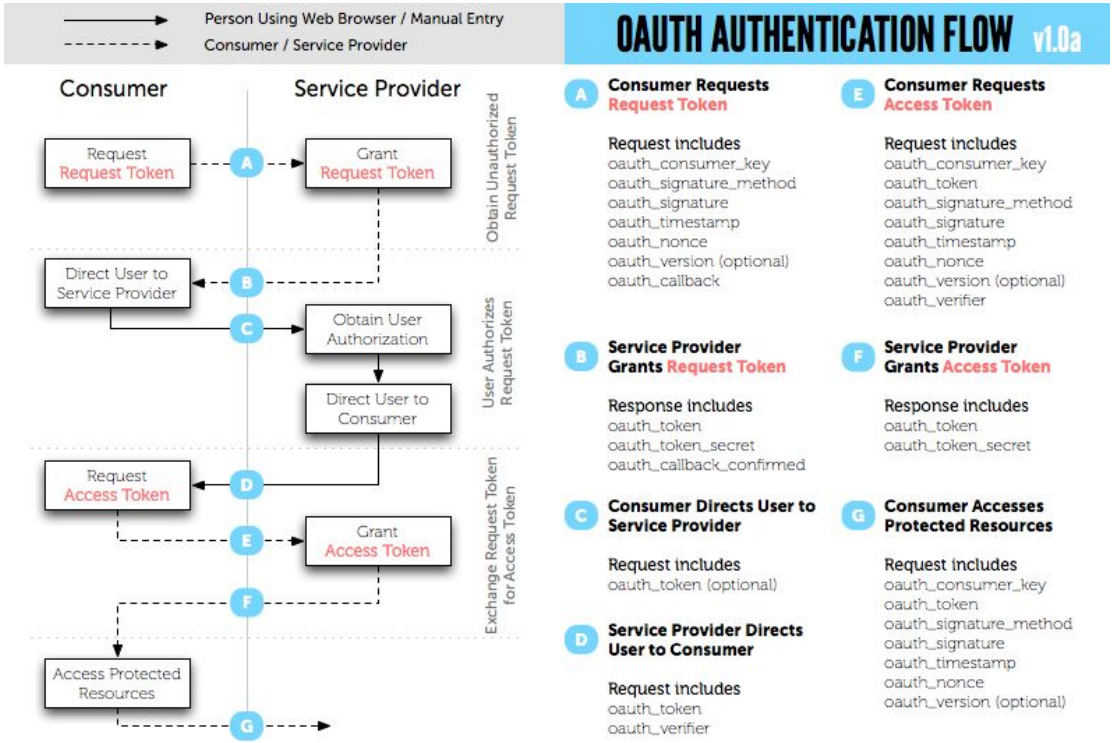
PRE-OAUTH ERA

Google calendar

PRE-OAUTH ERA

- Google ClientLogin / AuthSub
- Flickr Auth
- Yahoo BBAuth

OAUTH 1.0


Person Using Web Browser / Manual Entry
Consumer / Service Provider
OAUTH AUTHENTICATION FLOW v1.0a
Consumer
Service Provider
Request Request Token
Grant Request Token
Obtain Unauthorized Request Token
Direct User to Service Provider
Obtain User Authorization
Direct User to Consumer
User Authorizes Request Token
Request Access Token
Grant Access Token
Exchange Request Token for Access Token
Access Protected Resources
A Consumer Requests Request Token
Request includes
oauth_consumer_key
oauth_signature_method
oauth_signature
oauth_timestamp
oauth_nonce
oauth_version (optional)
oauth_callback
B Service Provider Grants Request Token
Response includes
oauth_token
oauth_token_secret
oauth_callback_confirmed
C Consumer Directs User to Service Provider
Request includes
oauth_token (optional)
D Service Provider Directs User to Consumer
Request includes
oauth_token
oauth_verifier
E Consumer Requests Access Token
Request includes
oauth_consumer_key
oauth_token
oauth_signature_method
oauth_signature
oauth_timestamp
oauth_nonce
oauth_version (optional)
oauth_verifier
F Service Provider Grants Access Token
Response includes
oauth_token
oauth_token_secret
G Consumer Accesses Protected Resources
Request includes
oauth_consumer_key
oauth_token
oauth_signature_method
oauth_signature
oauth_timestamp
oauth_nonce
oauth_version (optional)

OAUTH WRAP

- In Nov 2009, OAuth WRAP was introduced as a draft specification for access delegation, built on top of OAuth 1.0.
- WRAP was later deprecated in favour of OAuth 2.0.
- WRAP is not based on a signature scheme (like OAuth 1.0)
- In 2009, Facebook add OAuth WRAP support FriendFind.
- Introduced multiple profiles (autonomous client profiles and user delegation profiles).
- Client Account & Password / Assertion / Username & Password / Web App / Rich App profiles.

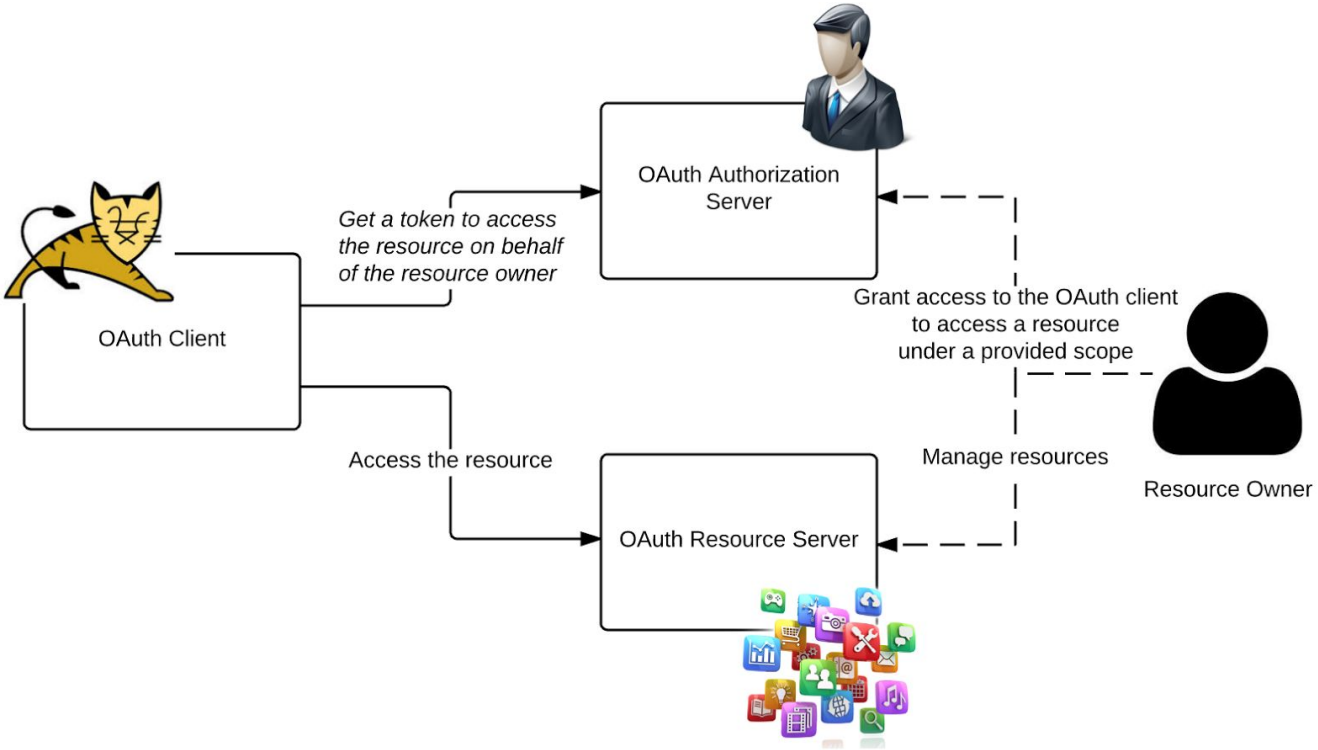
OAUTH 2.0

- The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

OAUTH 1.0 vs. OAUTH 2.0

- OAuth 1.0 is a concrete protocol for access delegation, while OAuth 2.0 is an authorization framework.
- OAuth 1.0 is signature based (HMAC-SHA256, RSA-SHA256) - while OAuth 2.0 supports multiple token profiles.
- OAuth 1.0 is less extensible.
- OAuth 1.0 is less developer friendly.
- OAuth 1.0 requires TLS only for the initial handshake - but OAuth 2.0 requires TLS through the flow.

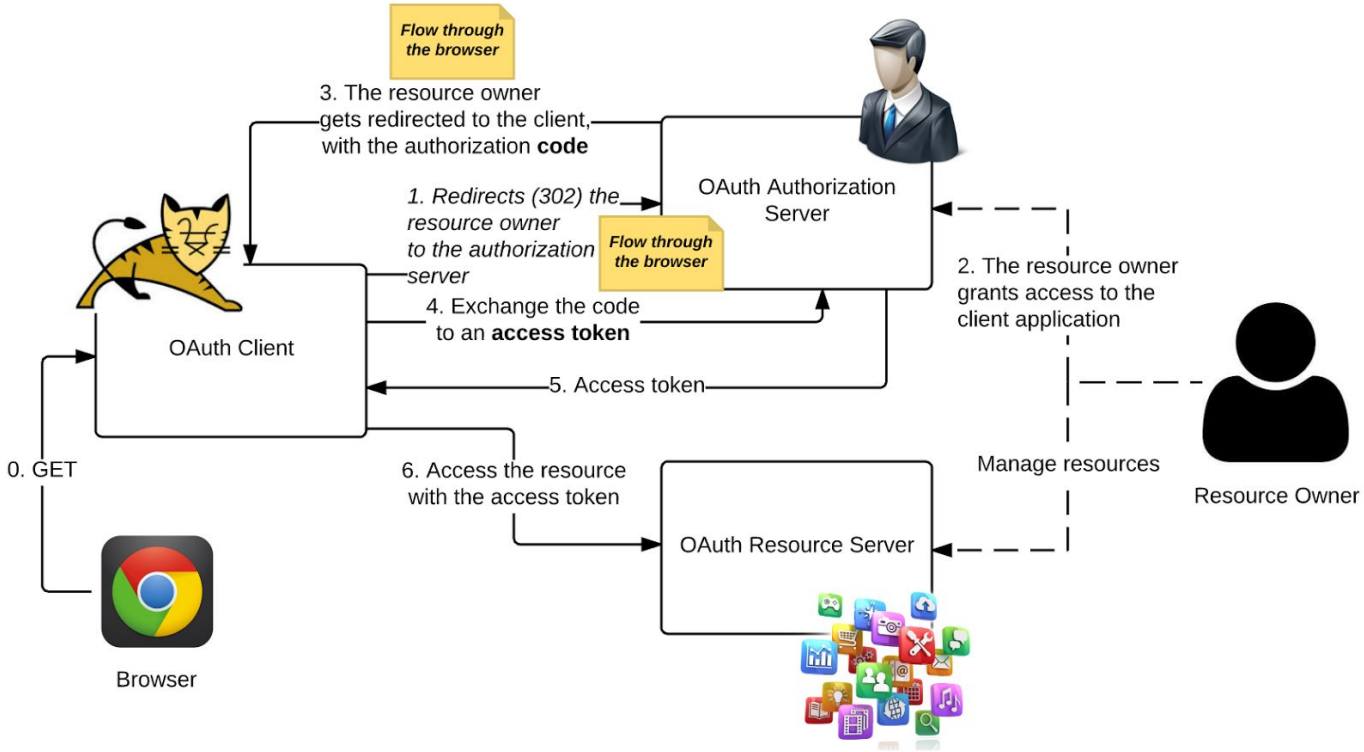
OAUTH 2.0


OAuth Authorization Server
Get a token to access the resource on behalf of the resource owner
OAuth Client
Grant access to the OAuth client to access a resource under a provided scope
Resource Owner
Access the resource
Manage resources
OAuth Resource Server

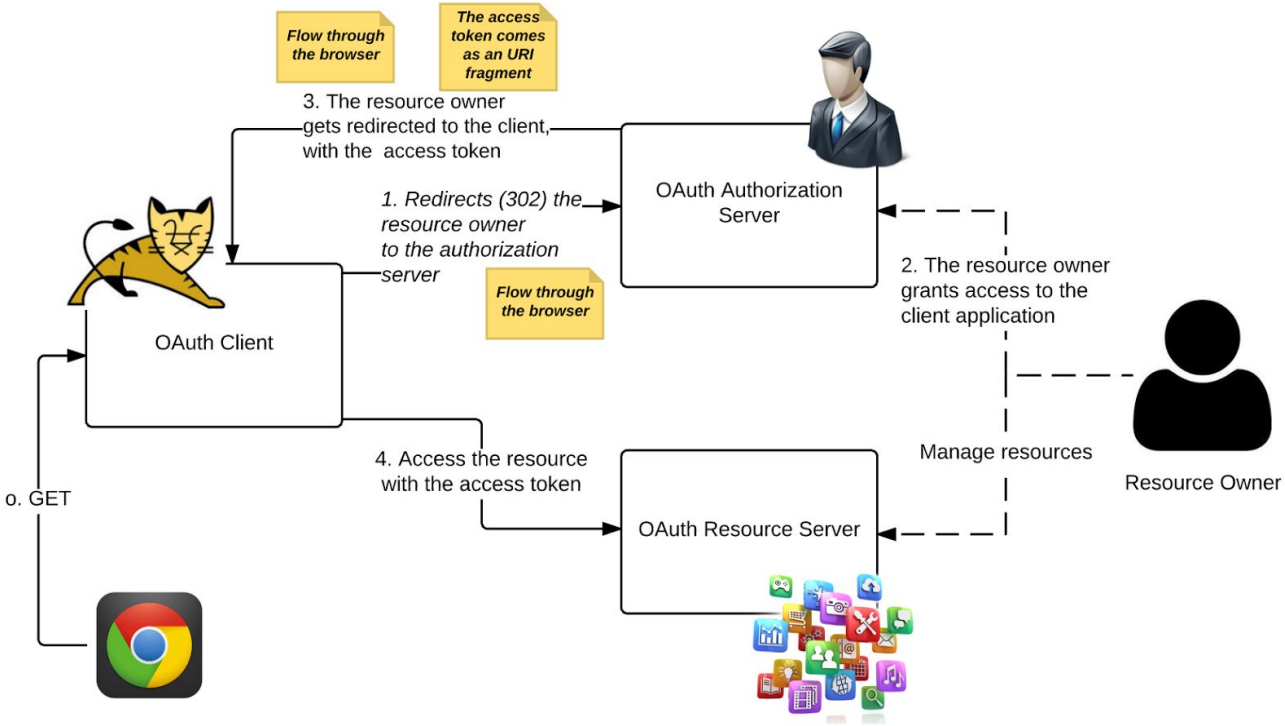
GRANT TYPES

- A grant type defines how a client could obtain an authorization grant from the authorization server on behalf of the resource owner.
- A grant type is a powerful extension point in OAuth 2.0.

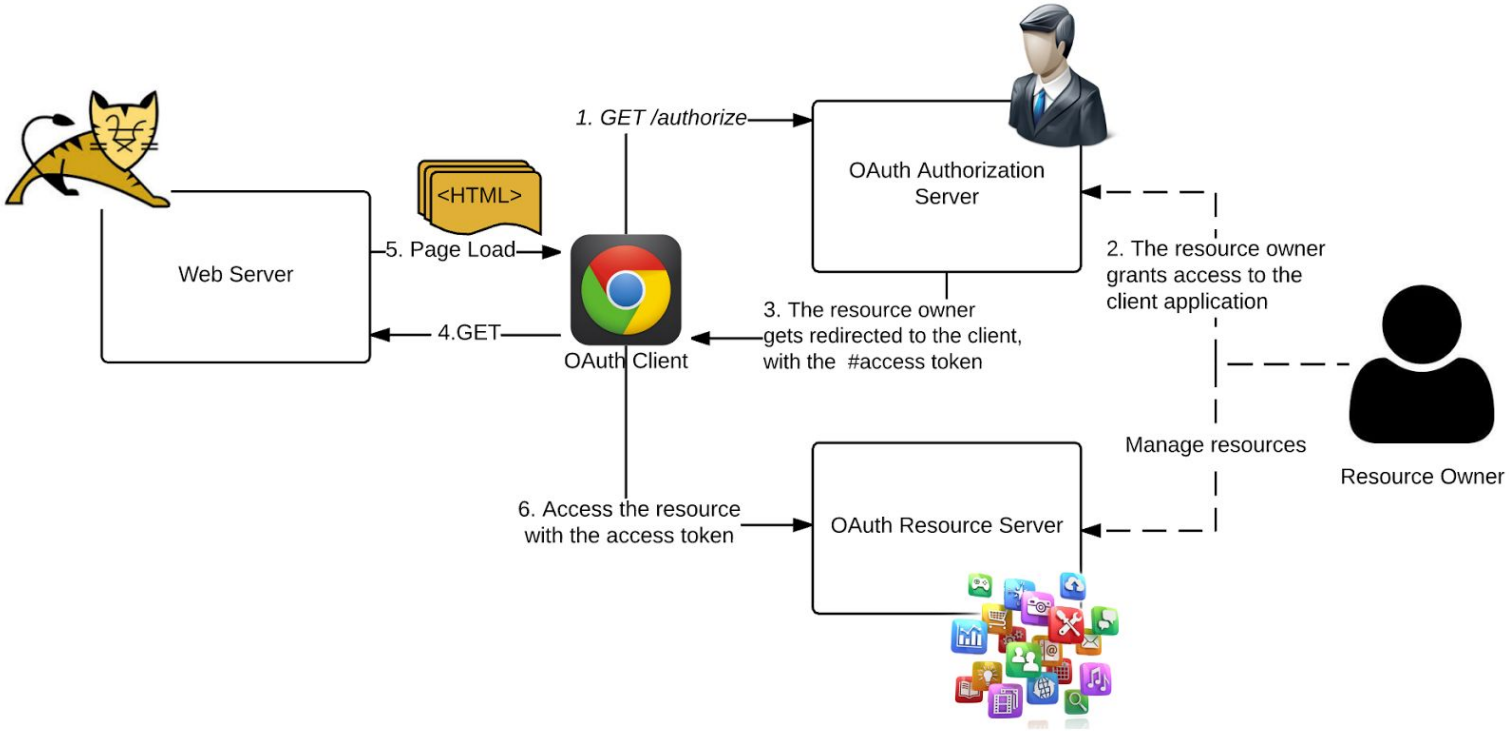
AUTHORIZATION CODE GRANT TYPE



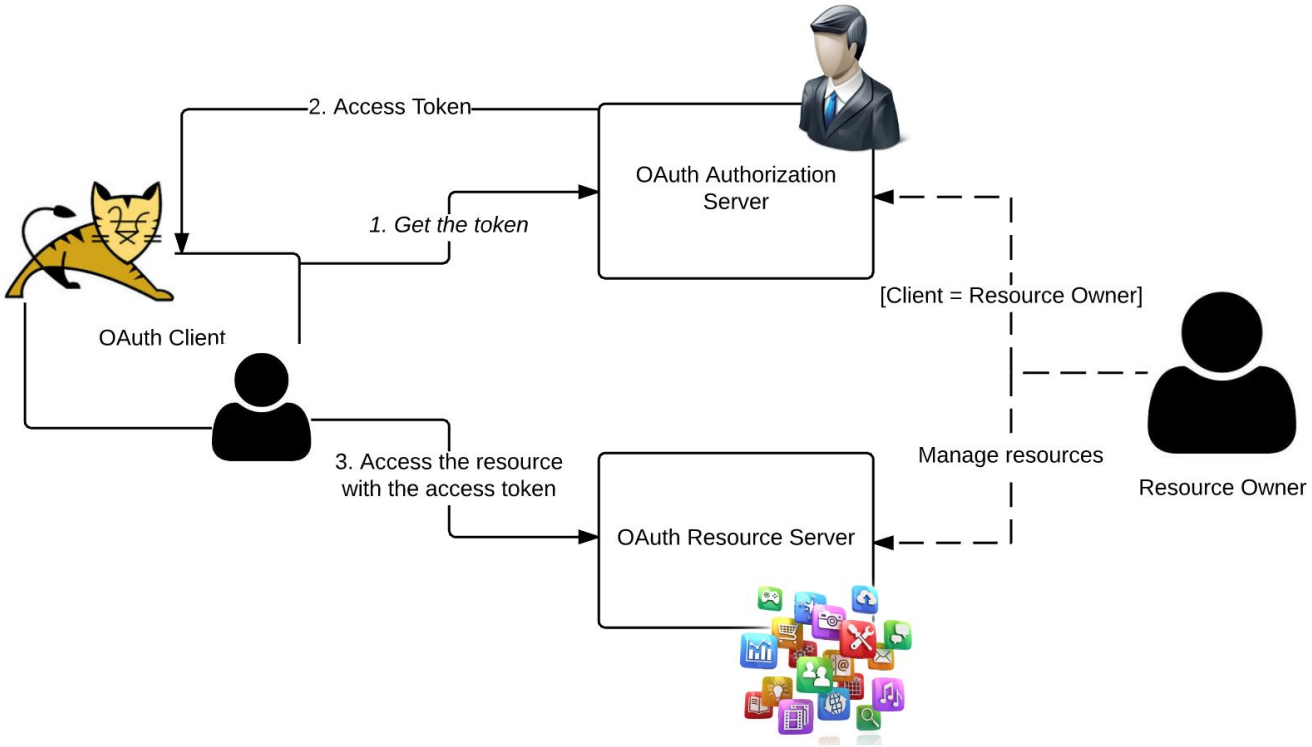
IMPLICIT GRANT TYPE (I)



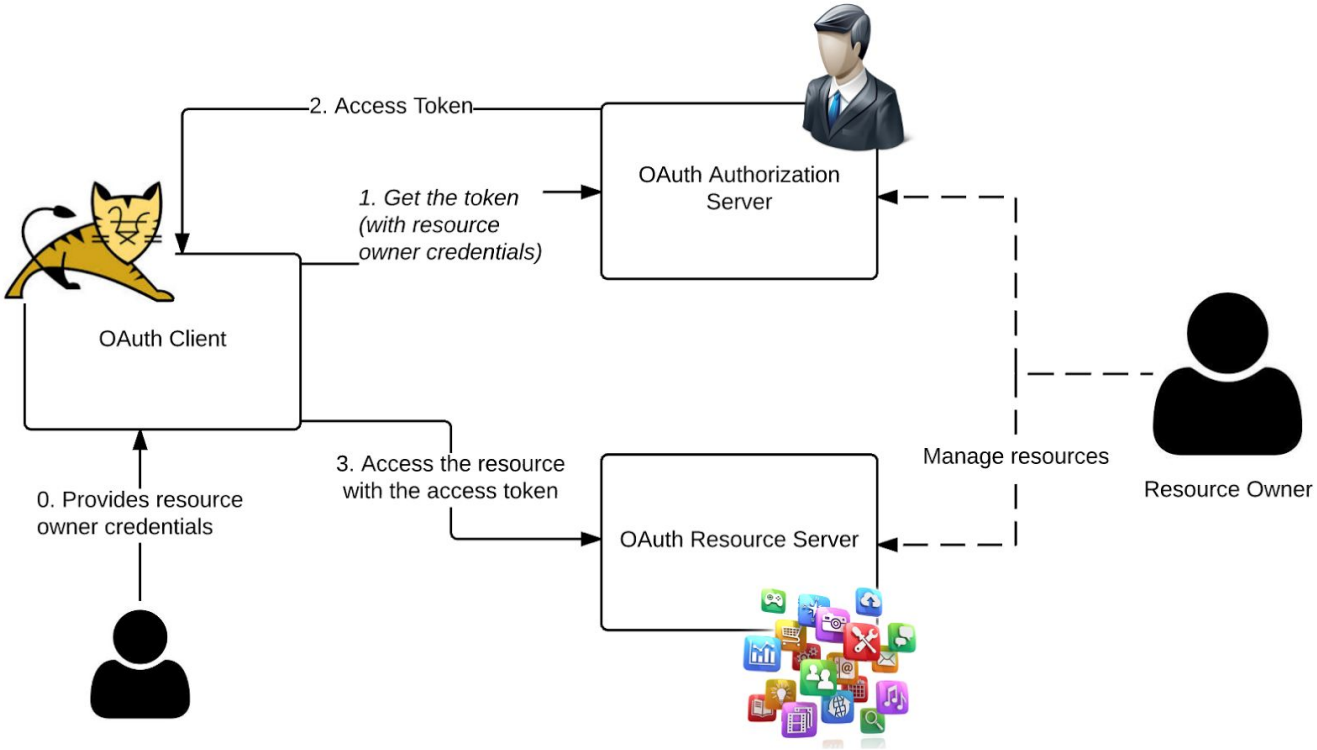
IMPLICIT GRANT TYPE (II)



CLIENT CREDENTIALS GRANT TYPE



PASSWORD GRANT TYPE



CREATE, PUBLISH & INVOKE API

- Deploy WSO2 API Manager
- Create an API against https://blockchain.info/ and publish
- Create an application
- Invoke API with password, client credentials, implicit and code grant types
- Check the behaviour of scope
- Observe the JWT being sent to the downstream service from the API gateway
- Check the behavior of different throttle limits

SCOPE

- Defines the scope of the access token - what can be done with the access token.
- The authorization and token endpoints allow the client to specify the scope of the access request using the "scope" request parameter.
- In turn, the authorization server uses the "scope" response parameter to inform the client of the scope of the access token issued.
- The value of the scope parameter is expressed as a list of space- delimited, case-sensitive strings.

TOKEN TYPES

- Neither OAuth 1.0 nor WRAP supported custom token types.
- OAuth 2.0 does not mandate any token type.
- OAuth 2.0 Bearer Token / OAuth 2.0 MAC Token
- Almost all the OAuth 2.0 deployments are based on Bearer token profile.

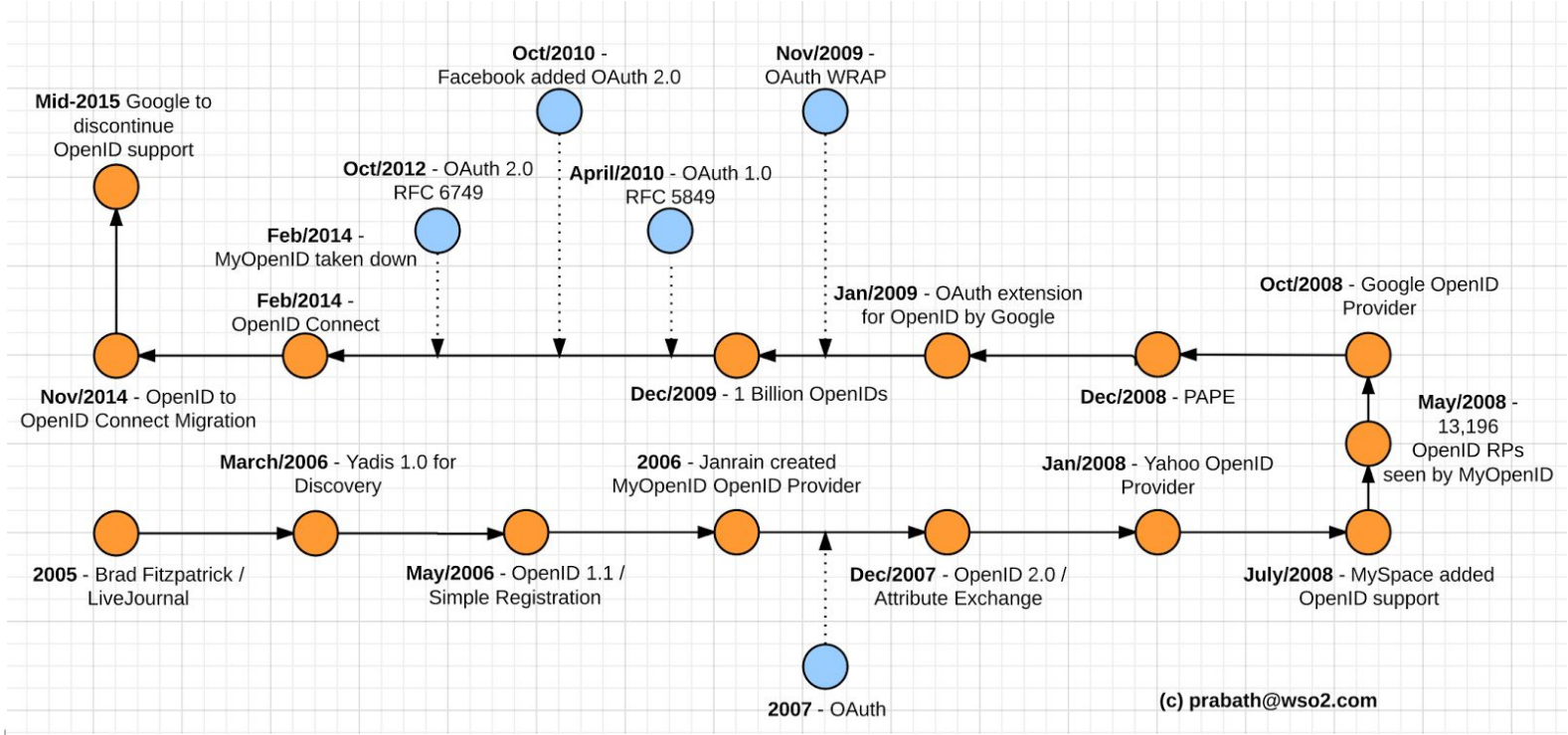
CLIENT TYPES

- OAuth 2.0 identifies two types of clients: confidential clients and public clients.
- A confidential client is capable of protecting its own credentials while not a public client.
- Web app is a confidential client, while a native mobile app and an SPA are public clients.

OPENID CONNECT (OIDC)

- An identity layer on top of the OAuth 2.0.
- Enables clients to verify the identity of the end-user based on the authentication performed by an Authorization Server.
- Use to obtain basic profile information about the End-User in an interoperable and REST-like manner.

OPENID CONNECT (OIDC)



JWT

JWT (JSON WEB TOKEN)

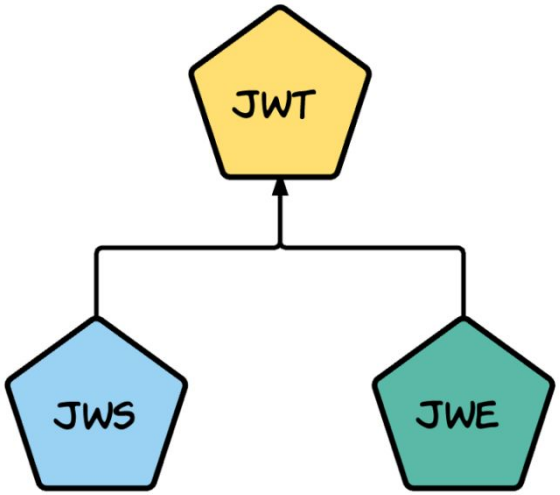
- Defines a container to transport data between interested parties.
- There are multiple applications of JWT - in OpenID Connect the id_token is represented as a JWT.
- Propagate one's identity between interested parties.
- Propagate user entitlements between interested parties.
- Transfer data securely between interested parties over a unsecured channel.
- Assert one's identity, given that the recipient of the JWT trusts the asserting party.

JWT (JSON WEB TOKEN)

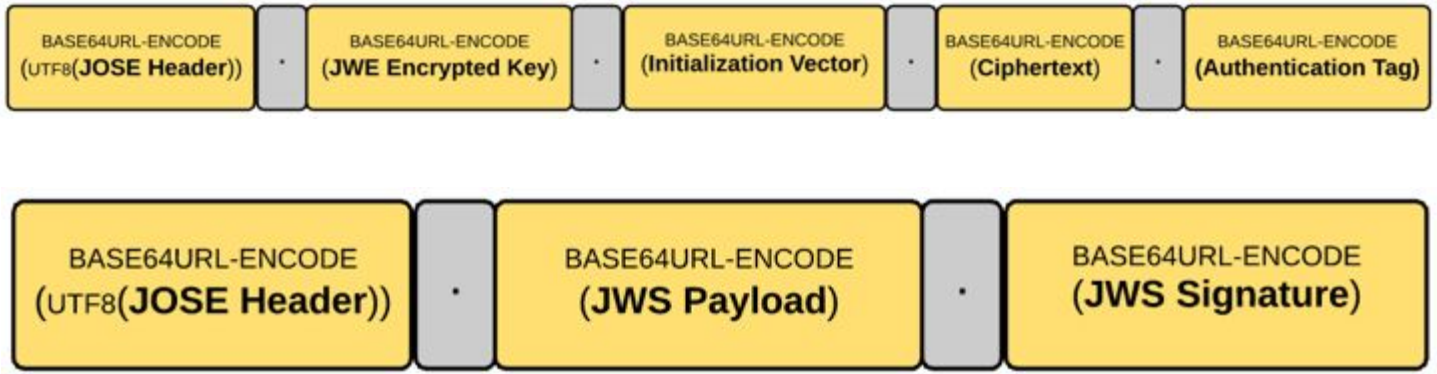
eyJhbGciOiJSUzI1NiIsImtpZCI6Ijc4YjRjZjIzNjU2ZGMzOTUzNjRmMWI2YzAyOTA3NjkxZjJjZGZmZTEifQ.eyJpc3MiOiJhY2NvdW50cy5nb29nbGUuY29tIiwic3ViIjoiMTEwNTAyMjUxMTU4OTIwMTQ3NzMyIiwiYXpwIjoiODI1MjQ5ODM1NjU5LXRlOHFnbDcwMWtnb25ub21ucDRzcXY3ZXJodTEyMTFzLmFwcHMuZ29vZ2xldXNlcmNvbnRlbnQuY29tIiwiZW1haWwiOiJwcmFiYXRoQHdzbzIuY29tIiwiYXRfaGFzaCI6InpmODZ2TnVsc0xCOGdGYXFSd2R6WWciLCJlbWFpbF92ZXJpZmllZCI6dHJ1ZSwiYXVkIjoiODI1MjQ5ODM1NjU5LXRlOHFnbDcwMWtnb25ub21ucDRzcXY3ZXJodTEyMTFzLmFwcHMuZ29vZ2xldXNlcmNvbnRlbnQuY29tIiwiaGQiOiJ3c28yLmNvbSIsImlhdCI6MTQwMTkwODI3MSwiZXhwIjoxNDAxOTEyMTcxfQ.**TVKv-pdyvk2gW8sGsCbsnkqsrS0T-H00xnY6ETklfglxfotvFn5IwKm3xyBMpy0FFe0Rb5Ht8AEJV6PdWyxz8rMgX2HROWqSo_RfEfUpBb4iOsq4W28KftW5H0lA44VmNZ6zU4YTqPSt4TPhyFC9fP2D_Hg7JQozpQRUfbWTJI**

JWT (JSON WEB TOKEN)

- A JWT does not exist itself — either it has to be a JWS or a JWE (JSON Web Encryption).
- It's like an abstract class — the JWS and JWE are the concrete implementations.
- We call a JWS or JWE, a JWT only if it follows the compact serialization.



JWT (JSON WEB TOKEN)

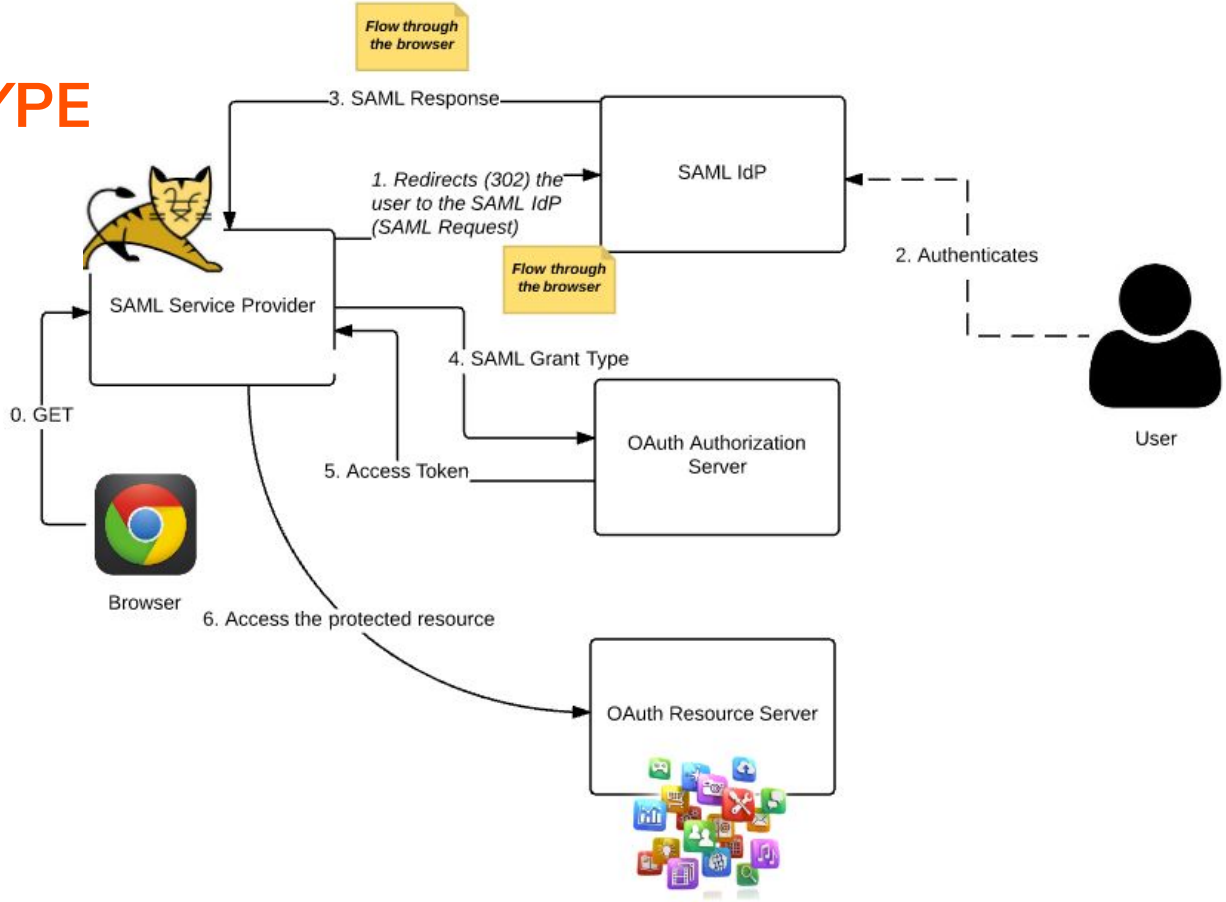


JWT, JWS, JWE

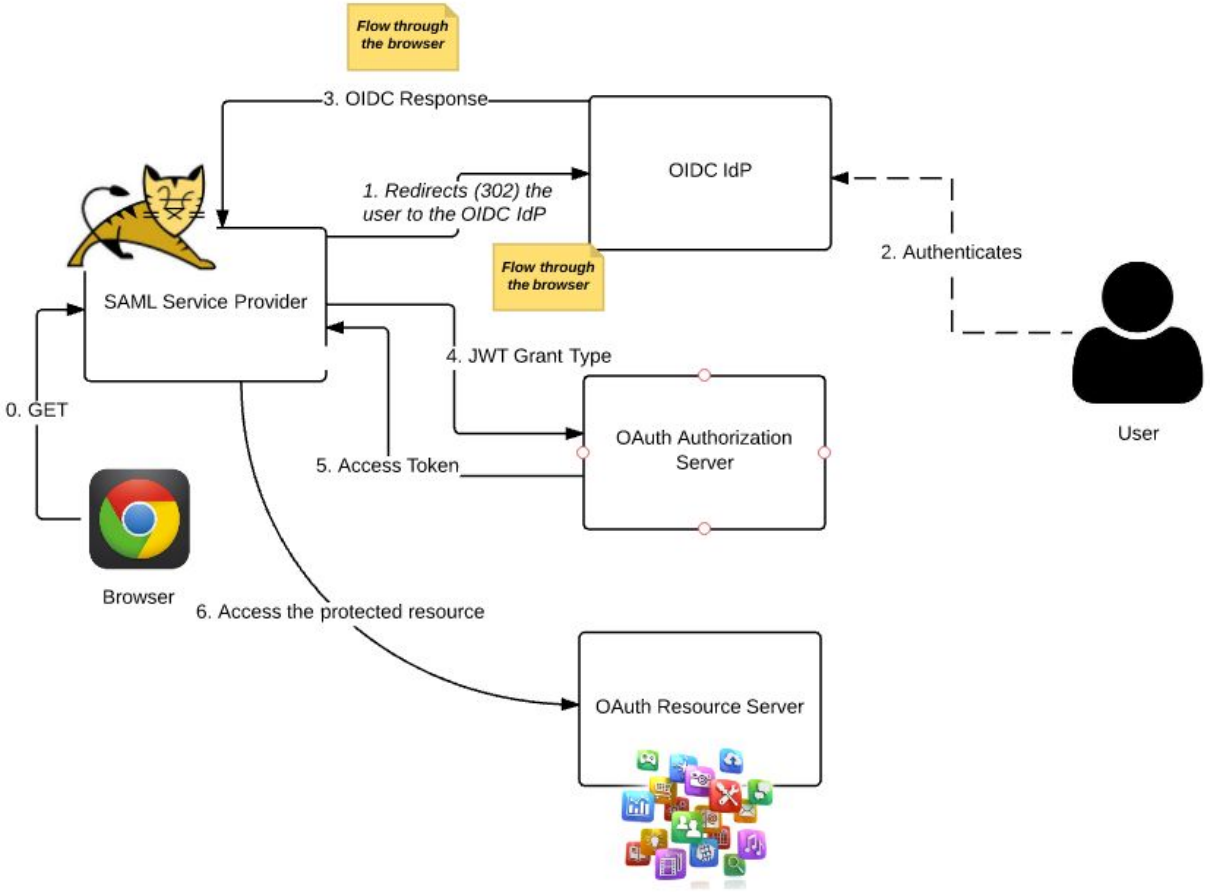
- Create JWS/JWE with Java Nimbus library - HMACSHA256 / RSAOAEP
- https://docs.wso2.com/display/ISCONNECTORS/JWT+Grant+Type+for+OAuth2

FEDERATED API ACCESS PATTERNS

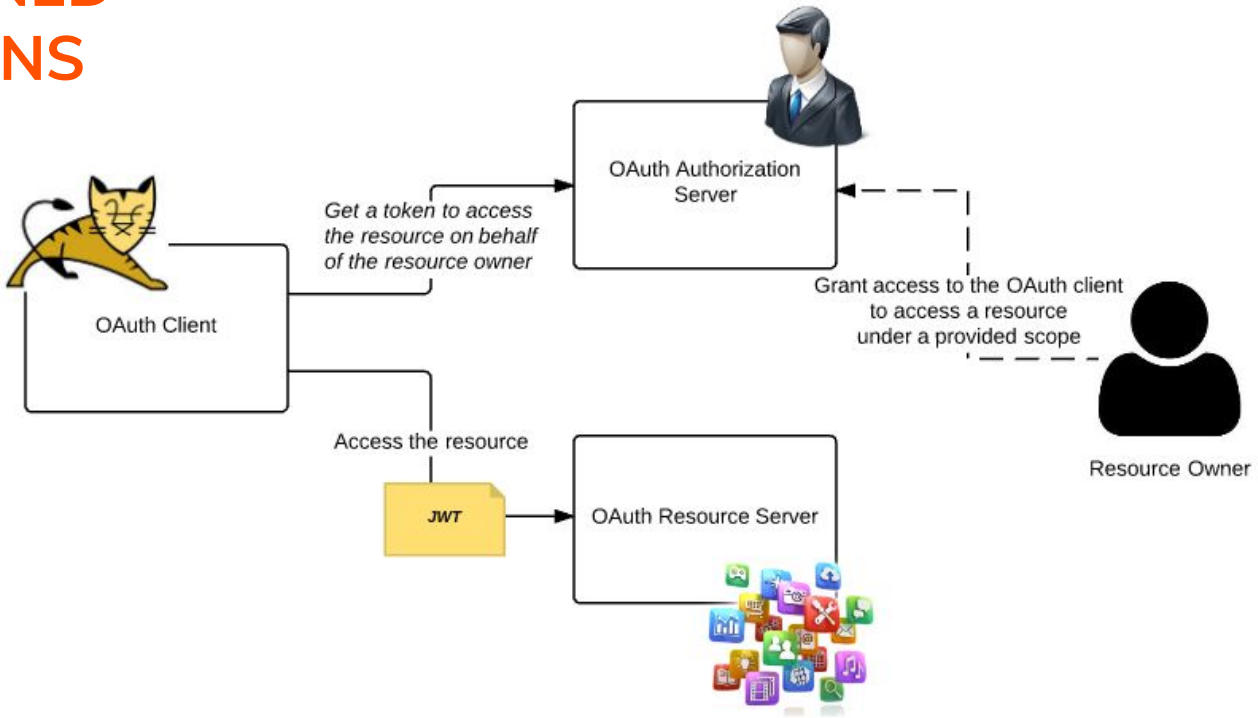
SAML GRANT TYPE FOR OAUTH 2.0



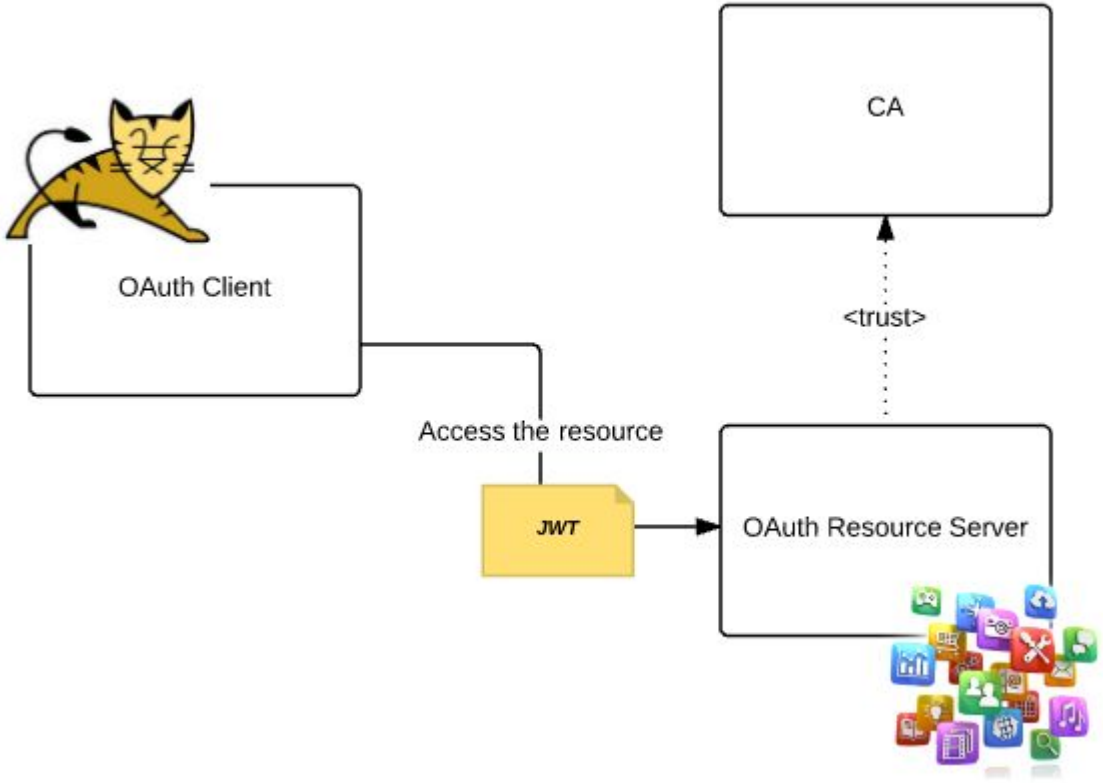
JWT GRANT TYPE FOR OAUTH 2.0



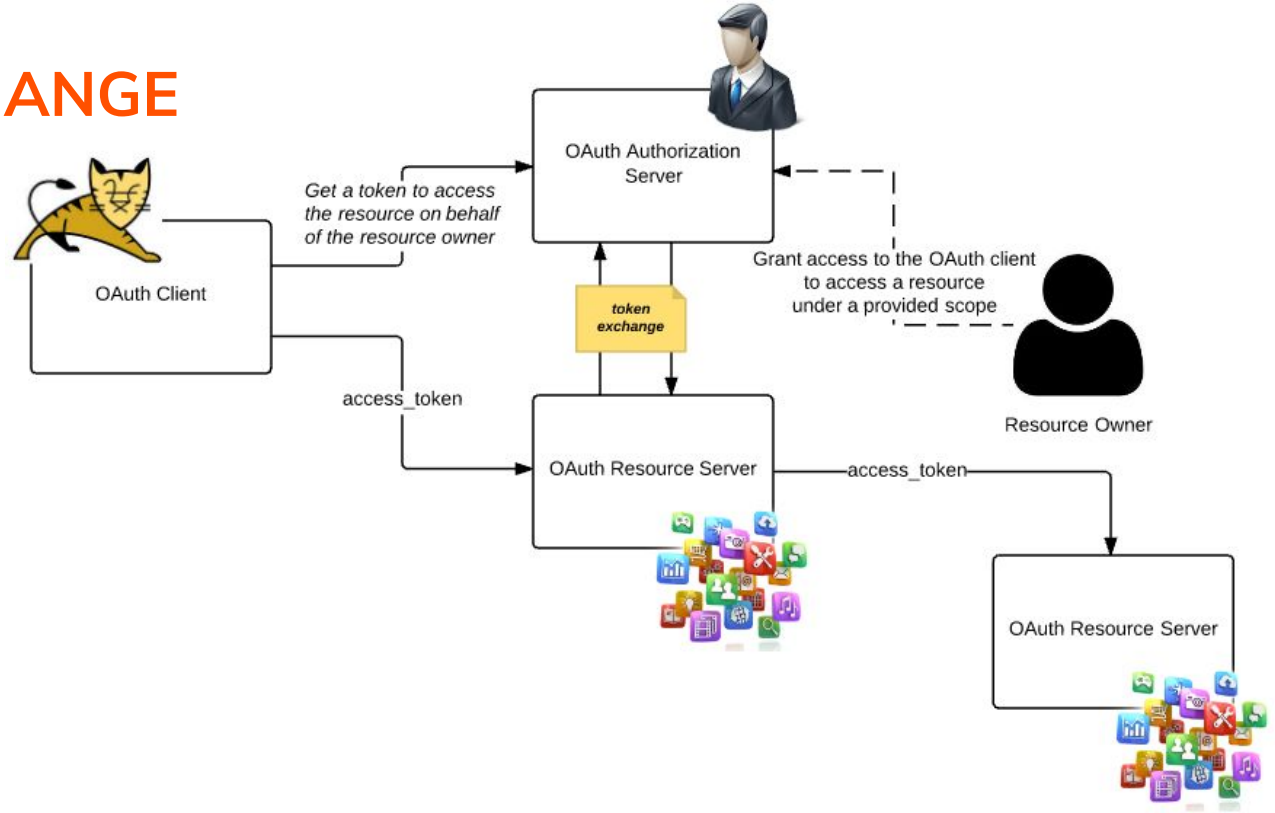
SELF-CONTAINED ACCESS TOKENS



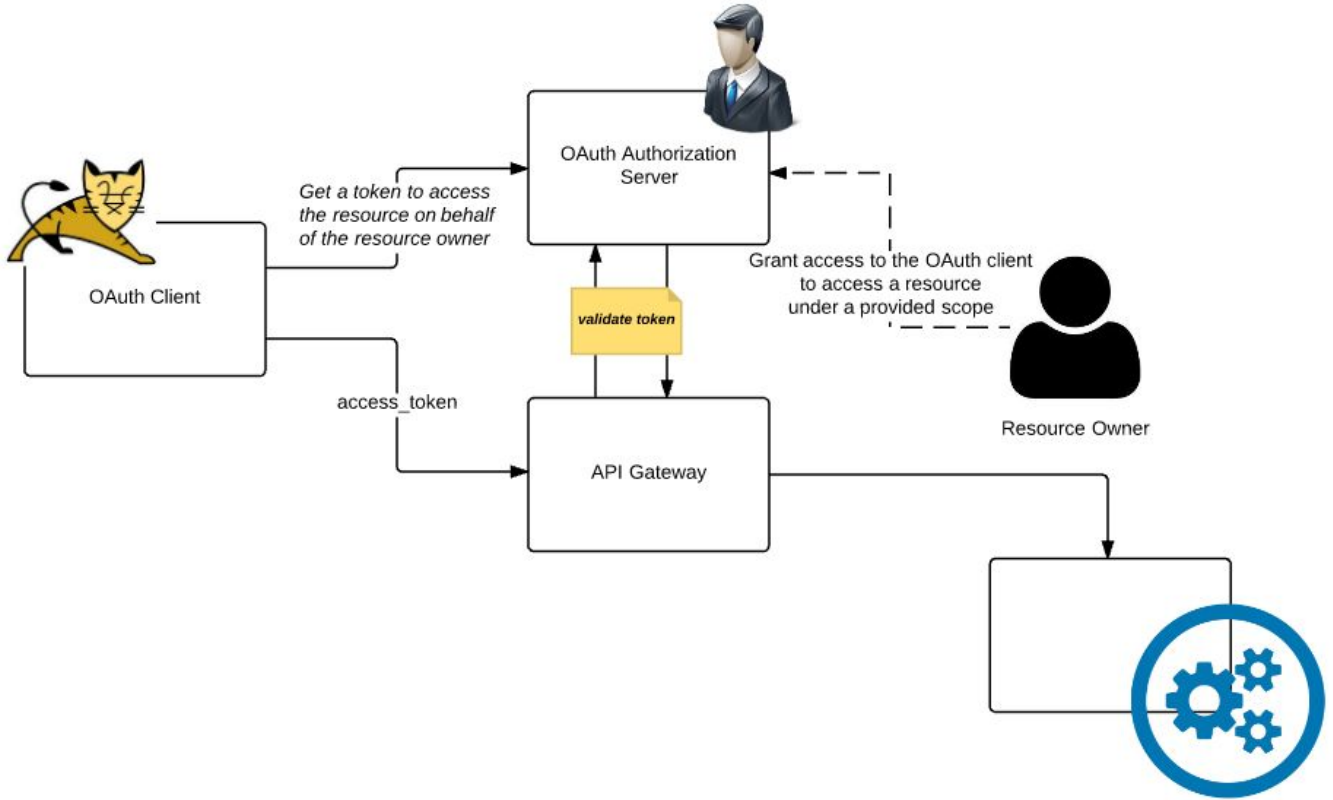
SELF ISSUED ACCESS TOKENS



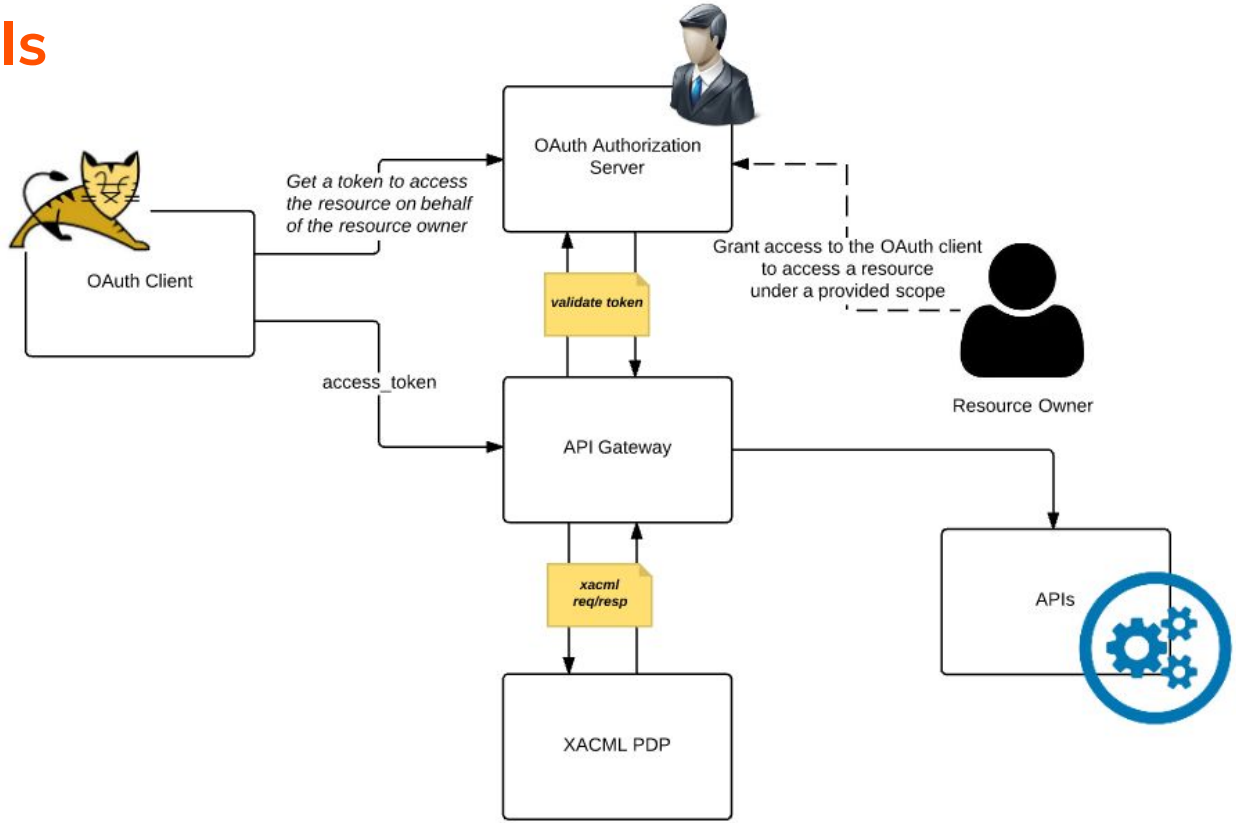
OAUTH 2.0
TOKEN EXCHANGE



API GATEWAY PATTERN



Fine-grained Access Control for APIs



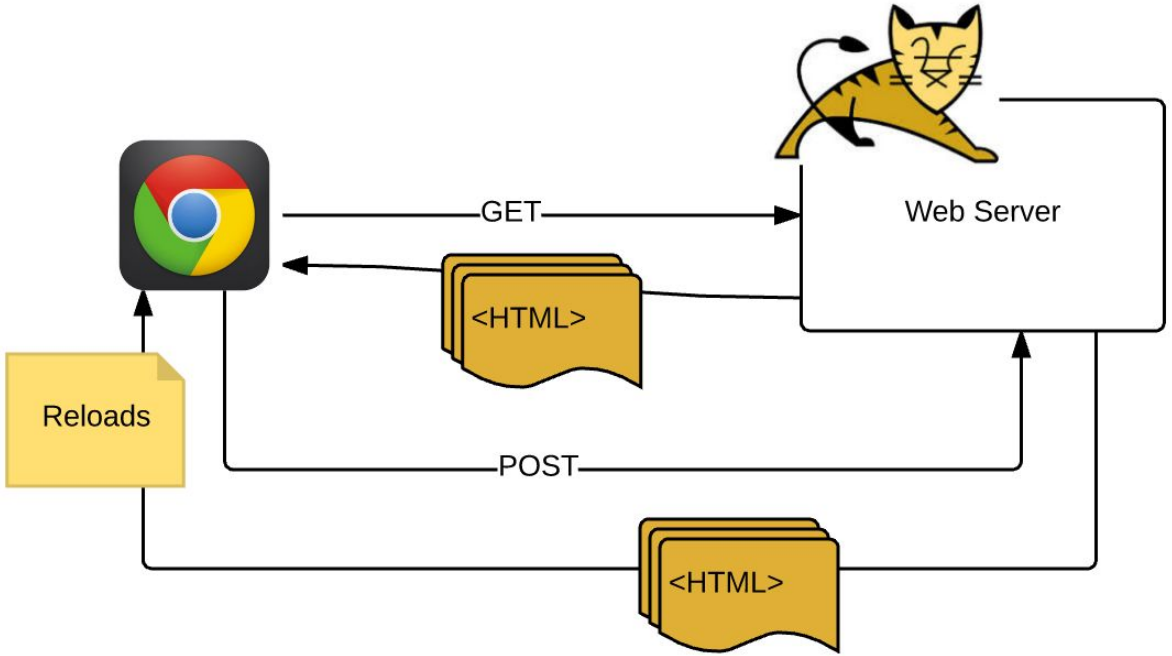
SINGLE PAGE APPLICATIONS

SINGLE PAGE APPLICATIONS

- Single-Page Applications (SPAs) are Web apps that load a single HTML page and dynamically update that page as the user interacts with the app.
- An SPA is an application delivered to the browser that doesn't reload the page during use.
- SPAs use AJAX and HTML5 to create fluid and responsive Web apps, without constant page reloads.
- The "page" in SPA is the single web page that the server sends to the browser when the application starts. It's the server rendered HTML that gets everything started. No more, no less. After that initial page load, all of the presentation logic is on the client.
- Much of the work happens on the client side, in JavaScript.
- User Agent-based Application

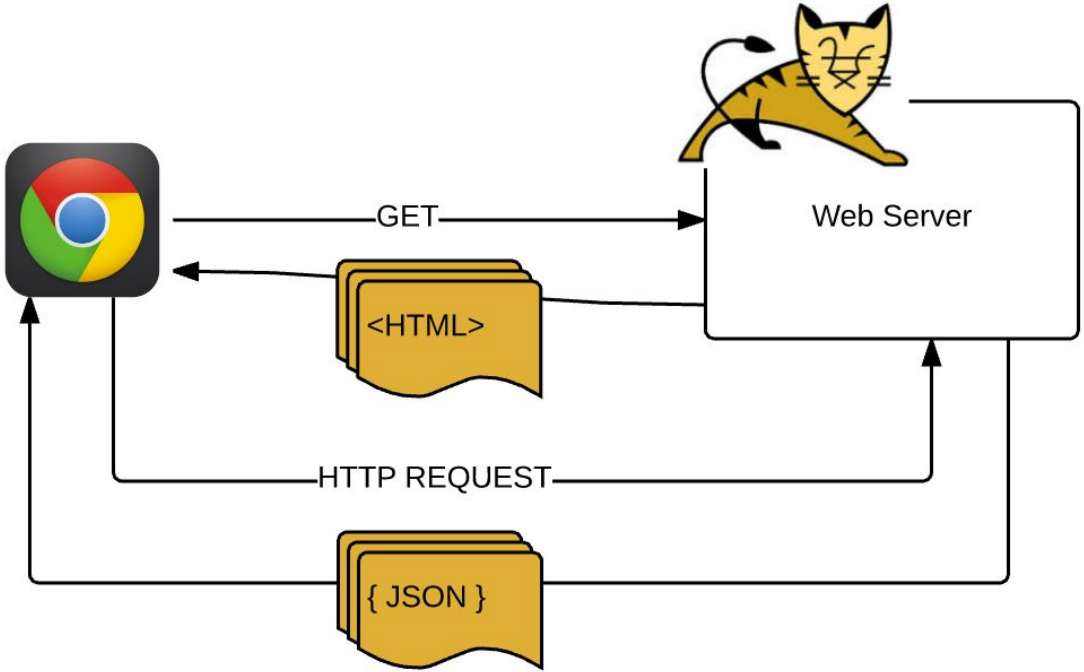
SINGLE PAGE APPLICATIONS

TRADITIONAL PAGE LIFECYCLE



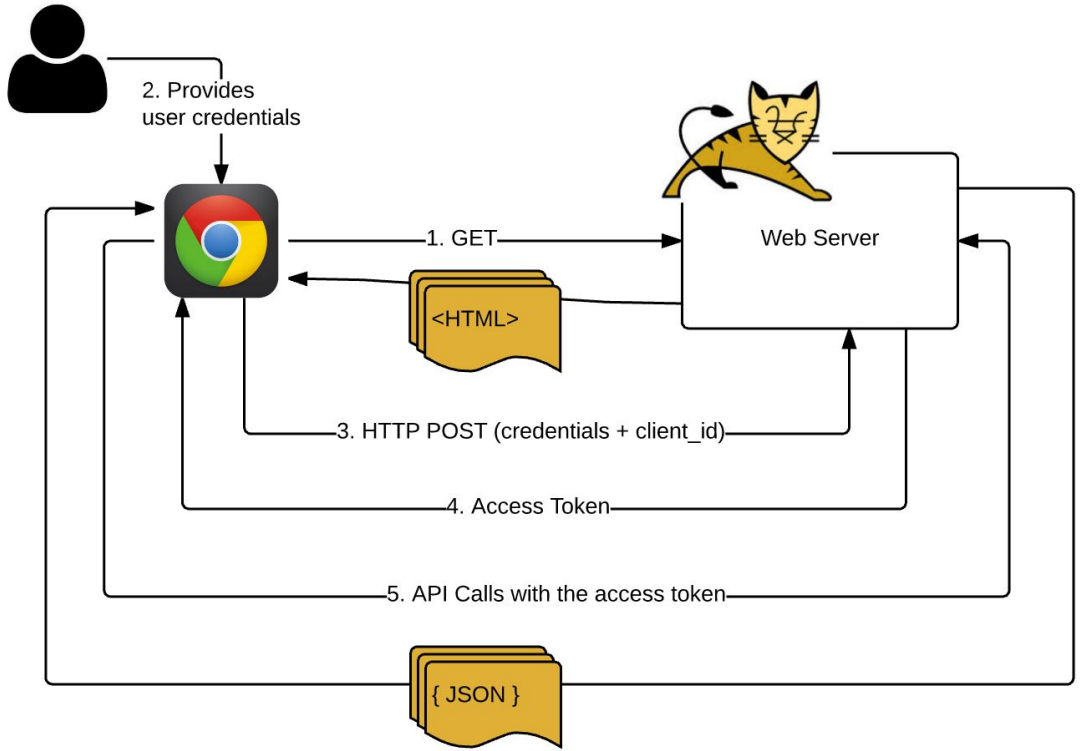
SINGLE PAGE APPLICATIONS

SPA LIFECYCLE



SECURING SPAs (I)

PASSWORD GRANT TYPE



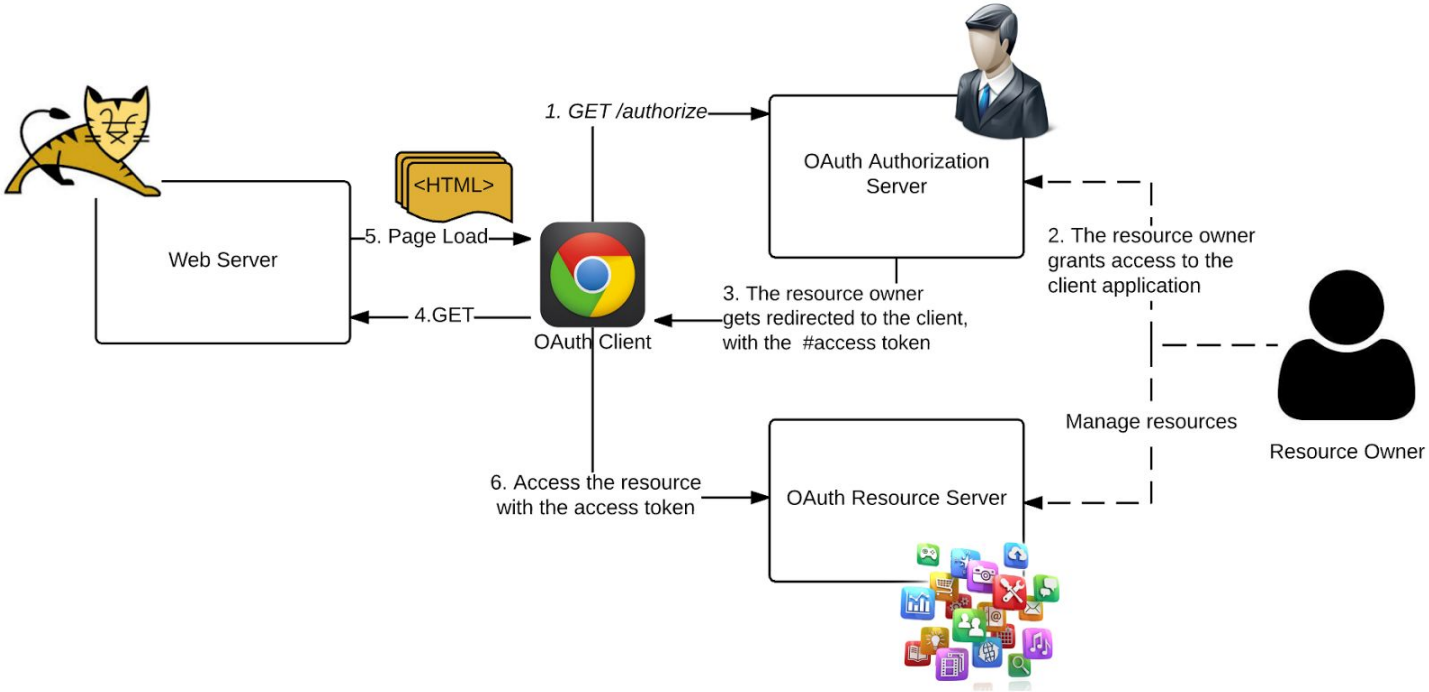
SECURING SPAs (I)

PASSWORD GRANT TYPE

- Two fundamental issues you find in any ‘pure’ SPA application.
  - *An SPA accessing an OAuth secured API is - the client cannot be authenticated in a completely legitimate manner.*
  - *An SPA accessing an OAuth secured API is - the access token cannot be made invisible to the end-user.*
- No single sign on experience.
- Users have to provide their credentials directly to the SPA - rather than to the identity provider. Must trust the SPA.
- No UI redirections.

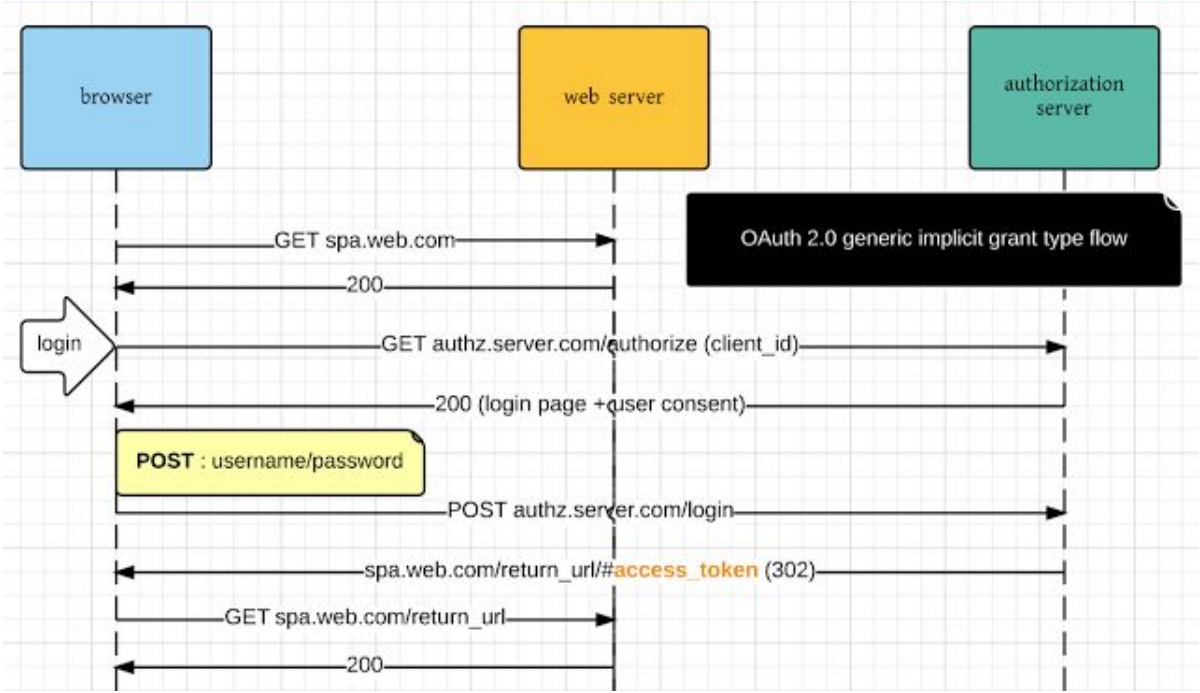
SECURING SPAs (II)

IMPLICIT GRANT TYPE



SECURING SPAs (II)

IMPLICIT GRANT TYPE



SECURING SPAs (II)

IMPLICIT GRANT TYPE

- Two fundamental issues you find in any ‘pure’ SPA application.
  - *An SPA accessing an OAuth secured API is - the client cannot be authenticated in a completely legitimate manner.*
  - *An SPA accessing an OAuth secured API is - the access token cannot be made invisible to the end-user.*
- Single sign on experience.
- Users do not need to provide credentials to the SPA, rather to the identity provider.
- UI redirections.

OVERCOMING SECURITY CHALLENGES

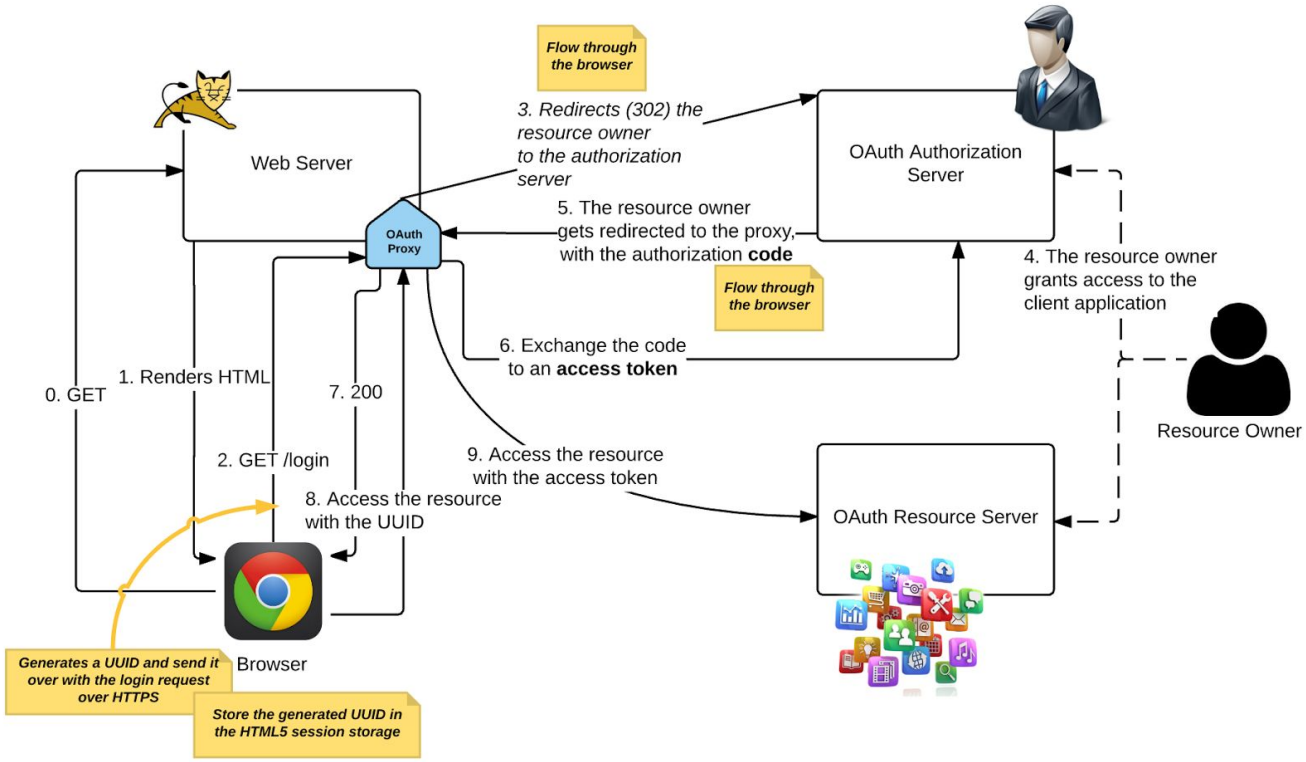
- An SPA accessing an OAuth secured API and the client cannot be authenticated in a completely legitimate manner.
  - Impact
    - Invoke APIs protected with client_credentials grant type.
    - Impersonate a legitimate client application and fool the user to get his consent to access user resources on behalf of the legitimate user.
  - Recommendations
    - Reject any tokens used to access APIs, which are issued under client_credentials grant type.
    - The authorization should do proper validations on the redirect_url.

OVERCOMING SECURITY CHALLENGES

- An SPA accessing an OAuth secured API and the access token cannot be made invisible to the end-user.
  - Impact
    - Can eat-out throttling limits associated with an API per application.
    - Access token returned backed from the implicit grant type is in browser history. Can be used by illegitimate users.
  - Recommendations
    - Enforce per user per application throttling limits.
    - Make the access tokens short-lived.
    - One time access token - discard the access token in its first use (access token chaining).

SECURING SPAs (III)

OAuth Proxy



SECURING SPAs (II)

OAuth Proxy

- ~~Two fundamental issues you find in any 'pure' SPA application.~~
  - ~~*An SPA accessing an OAuth secured API is - the client cannot be authenticated in a completely legitimate manner.*~~
  - ~~*An SPA accessing an OAuth secured API is - the access token cannot be made invisible to the end-user.*~~
- Single sign on experience.
- Users do not need to provide credentials to the SPA, rather to the identity provider.
- UI redirections.
- Not pure SPA - all the API calls from the SPA should go through the SPA.

SECURING SPAs (IV)

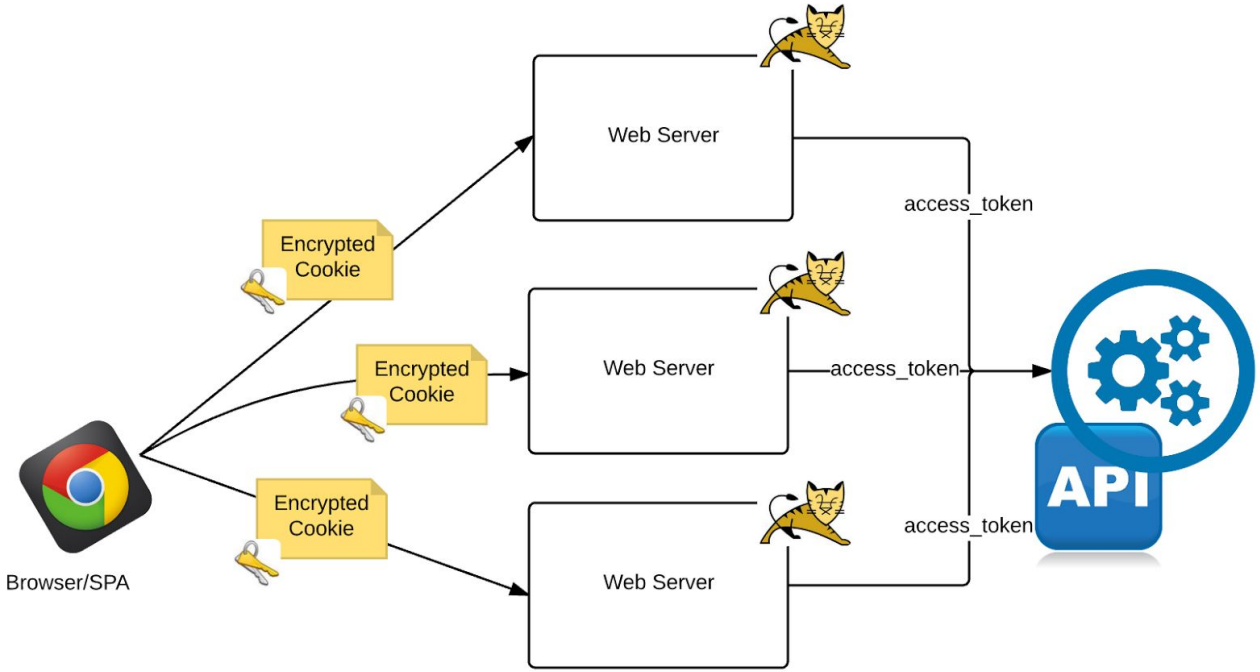
Stateless OAuth Proxy

- Create a JWE with the access token, user info - encrypt and set it in a session cookie, in the response to the login
- All the API calls from the SPA to the proxy, this cookie will be included.

```
 var xmlHttp = new XMLHttpRequest();
      xmlHttp.withCredentials = true;
      xmlHttp.onreadystatechange = function() {
            if (xmlHttp.readyState == 4 && xmlHttp.status == 200) {
                  var obj = JSON.parse(xmlHttp.responseText);
                  document.getElementById('name-id').innerHTML = obj.sub;
            }
};
xmlHttp.open("GET",
                  "https://localhost:9443/oauth2-proxy/users?code="
                        + sessionStorage.getItem("guid"), true);
xmlHttp.send();
```

SECURING SPAs (IV)

Stateless OAuth Proxy



NATIVE APPS

OAUTH 2.0 FOR NATIVE APPs

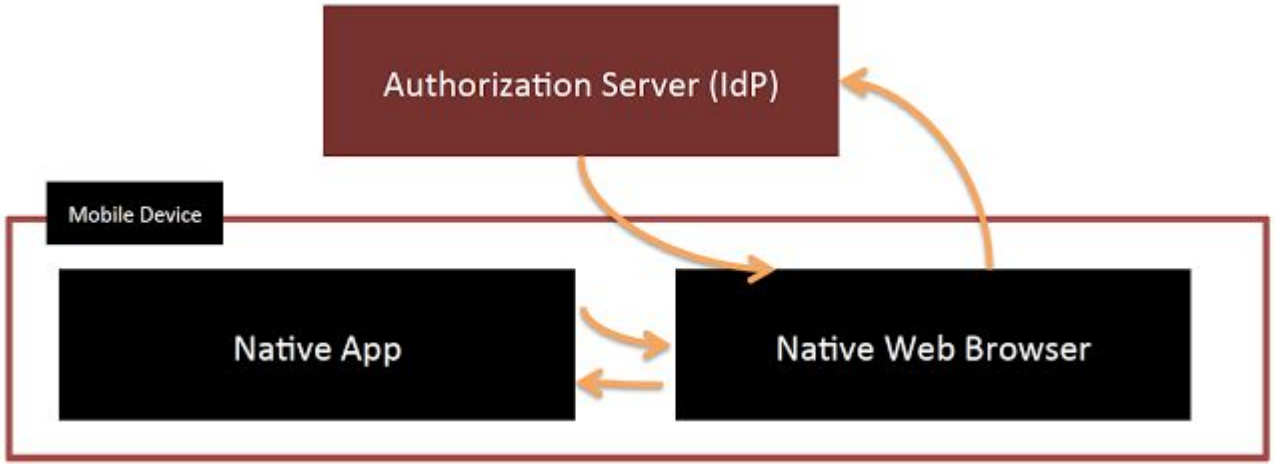
- Use the web view
- Session not shared among multiple native apps.
- Possible phishing attacks

OAUTH 2.0 FOR NATIVE APPs

- Use password grant type
- Session not shared among multiple native apps.
- Possible phishing attacks

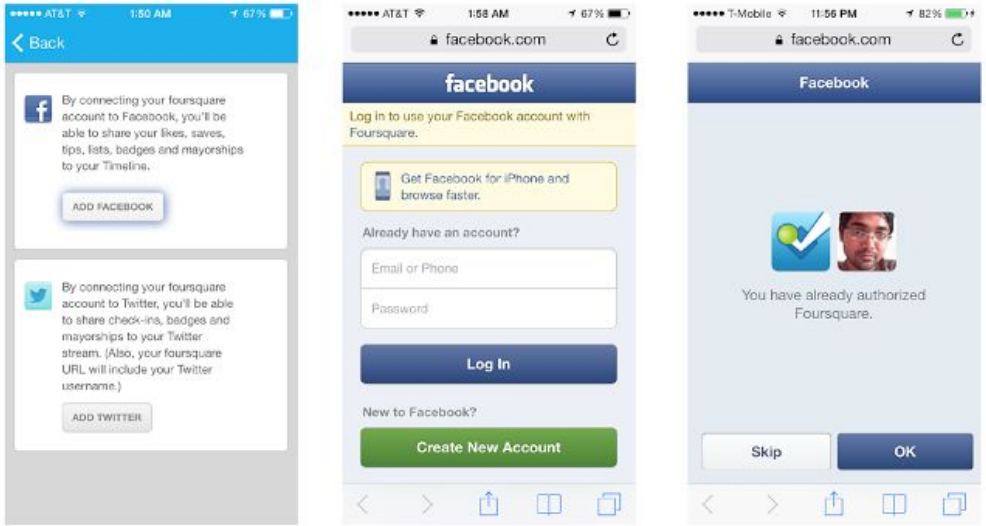
OAUTH 2.0 FOR NATIVE APPs

- Use the system browser
- Session shared among multiple native mobile apps



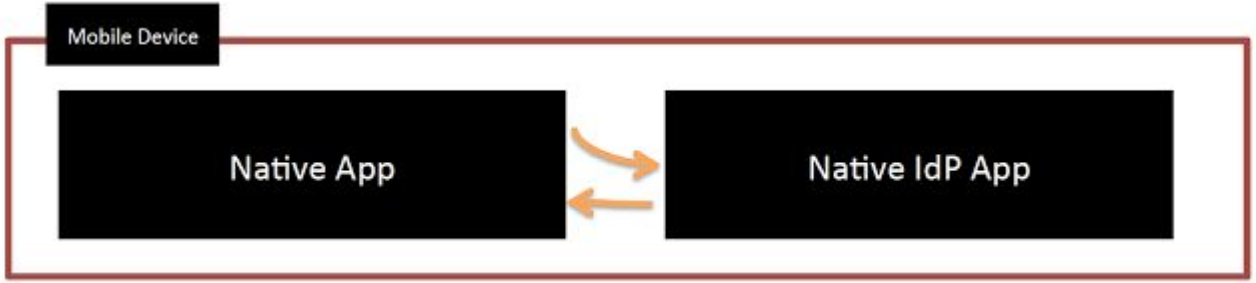
OAUTH 2.0 FOR NATIVE APPs

- Use the system browser
- Session shared among multiple native mobile apps



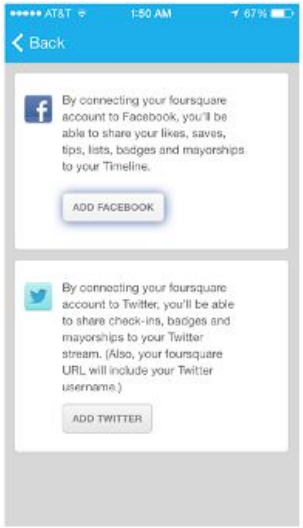
OAUTH 2.0 FOR NATIVE APPs

- Use an IdP proxy
- Session shared among multiple native apps
- NAPPS working group under OpenID foundation
- No more.



OAUTH 2.0 FOR NATIVE APPs

- Use an IdP proxy
- Session shared among multiple native apps
- NAPPS working group under OpenID foundation
- No more.



OAUTH 2.0 FOR NATIVE APPs

- Apple (iOS9+ - SFSafariViewController) and Google (Chrome 45+ - Chrome Custom Tabs)
- This web controller provides all the benefits of the native system browser in a control that can be placed within an application.
- Session shared between apps.

OAUTH 2.0 FOR NATIVE APPs

- The best practices draft under OAuth IETF working group ‘OAuth 2.0 for Native Apps’ recommends that OAuth 2.0 authorization requests from native apps should only be made through external user-agents, primarily the user's browser.

PKCE (PROOF KEY FOR CODE EXCHANGE)

- Authorization Code Grant are susceptible to the authorization code interception attack.
- The PKCE introduces a technique to mitigate against the threat.
- In this attack, the attacker intercepts the authorization code returned from the authorization endpoint within a communication path not protected by TLS.
- The attacker has access to the "client_id" and "client_secret" (if provisioned).
- Uses a cryptographically random string that is used to correlate the authorization request to the token request.

PKCE WITH OPENID CONNECT

- Using cURL

DYNAMIC CLIENT REGISTRATION PROFILE

- Defines mechanisms for dynamically registering OAuth 2.0 clients with authorization servers.
- The resulting registration responses return a client identifier to use at the authorization server and the client metadata values registered for the client.
- The client can then use this registration information to communicate with the authorization server using the OAuth 2.0 protocol.

TOKEN INTROSPECTION PROFILE

- Defines a method for a protected resource to query an OAuth 2.0 authorization server to determine the active state of an OAuth 2.0 token and to determine meta-information about this token.

```
POST /introspect HTTP/1.1
Host: server.example.com
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

token=mF_9.B5f-4.1JqM&token_type_hint=access_token
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{
        "active": true,
         "client_id": "l238j323ds-23ij4",
         "username": "jdoe",
         "scope": "read write dolphin",
        "sub": "Z5O3upPC88QrAjx00dis",
         "aud": "https://protected.example.net/resource",
         "iss": "https://server.example.com/",
         "exp": 1419356238,
        "iat": 1419350238,
        "extension_field": "twenty-seven"
}
```

TOKEN REVOCATION PROFILE

- Allows clients to notify the authorization server that a previously obtained refresh or access token is no longer needed

```
POST /revoke HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

token=45ghiukldjahdnhzdauz&token_type_hint=refresh_token
```

RESOURCE SET REGISTRATION PROFILE

- Defines a resource set registration mechanism between an OAuth 2.0 authorization server and resource server.
- A resource set is one or more resources that the resource server manages as a set, abstractly.
- A resource set may be a single API endpoint, a set of API endpoints, a classic web resource such as an HTML page.
- A set of scopes can be associated with a resource set during the registration.

THANK YOU

wso2.com